UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/889,524	02/28/2002	Dan Butnaru	09669/004001	5237

22511 7590 09/20/2004

OSHA & MAY L.L.P.
1221 MCKINNEY STREET
HOUSTON, TX 77010

EXAMINER
HENNING, MATTHEW T

ART UNIT	PAPER NUMBER
2131	9

DATE MAILED: 09/20/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/889,524	**Applicant(s)** BUTNARU ET AL.	
	Examiner Matthew T Henning	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 February 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *2-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *2-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *28 February 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *5*.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

This action is in response to the communication filed on 02/28/2002.

DETAILED ACTION

1. Claims 2-23 have been examined.

2. Claim 1 has been cancelled by the applicant and claims 20-23 have been added.

Title

3. The title of the invention is acceptable.

Priority

4. The application is a 371 of PCT/FR00/00099 filed 1/18/2000 claiming priority to France application 99/00462 filed on 01/18/1999.

5. The effective filing date for the subject matter defined in the pending claims in this application is 01/18/1999.

Information Disclosure Statement

6. The information disclosure statement (IDS) submitted on 02/28/2002 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the examiner is considering the information disclosure statement.

Drawings

7. The drawings filed on 02/28/2002 are acceptable for examination proceedings.

Specification

8. Applicant is reminded of the proper language and format for an abstract of the disclosure.

> *The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The*

abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

9. The abstract of the disclosure is objected to because

Line 1: "The present invention relates to" can be implied and therefore must be removed.

Lines 5 and 7 contain legal phraseology, which must be removed.

Lines 15-16: "The invention…banking field" refers to purported merits or speculative applications of the invention and must therefore be removed.

Correction is required. See MPEP § 608.01(b).

Claim Objections

10. The applicant is reminded that a series of singular dependent claims is permissible in which a dependent claim refers to a preceding claim which, in turn, refers to another preceding claim.

A claim which depends from a dependent claim should not be separated by any claim which does not also depend from said dependent claim. It should be kept in mind that a dependent claim may refer to any preceding independent claim. In general, applicant's sequence will not be changed. See MPEP § 608.01(n).

Claim Rejections - 35 USC § 112

11. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

12. Claims 5, 7, 16-19, and 22-23 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

13. The claims are generally narrative and indefinite, failing to conform with current U.S. practice. They appear to be a literal translation into English from a foreign document and are replete with grammatical and idiomatic errors.

14. Claim 5 recites the limitation "said information" in line 2, but fails to disclose which information this is referring to. The ordinary person skilled in the art would be unable to determine whether the application key is chosen based upon the "information pertaining to an application key", "information specific to the second unit", or "information comprising said operation key". Therefore, claim 5 fails to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

15. Claim 7 recites the limitation "verifying integrity of the data includes the encrypted application key" in line 2. This limitation is not grammatically correct, and as such, the examiner cannot discern the limitation proposed by this claim. For the purposes of searching art, the examiner will assume the claim meant that the integrity of the application key was verified at some point during the method.

16. Claims 16 and 17 recite the limitation "temporarily saved within the second volatile memory" in lines 2-3. There is insufficient antecedent basis for this limitation in the claims.

17. Claim 18 recites the limitation "the random information" in line 2. There is insufficient antecedent basis for this limitation in the claim.

18. Claim 19 recites the limitation “the information pertaining to an application key” in line 2. There is insufficient antecedent basis for this limitation in the claim.

19. Claim 22 recites the limitation "the random information" in line 2. There is insufficient antecedent basis for this limitation in the claim.

20. Claim 23 recites the limitation “the information pertaining to an application key” in line 2. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

21. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> *A person shall be entitled to a patent unless –*
>
> *(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.*

22. Claims 2–6, and 8-23 are rejected under 35 U.S.C. 102(b) as being anticipated by Moriyasu et al. (US Patent Number 5,651,066) hereinafter referred to as Moriyasu.

23. Claim 20 recites a method for customizing a set of several second security units (See Moriyasu Fig. 3 and Field of the Invention), comprising:

secure downloading of an application key from a first security unit of a central processing unit to said set of second security units (See Moriyasu Fig. 3 and Field of the Invention), said first unit and second units each comprising at least one memory (See Moriyasu Col. 7 Paragraph 8 wherein it was implied that the management units had memory because keys were stored there), wherein the method further comprises for each second unit in said set:

on each downloading (See Moriyasu Fig. 10), computing an operation key (K3'+K4) in the first unit based on information specific to the second unit (K3), a transport key (K4), and a diversification algorithm (Multi-Value Function) (See Moriyasu

Col. 8 Paragraph 6), said transport key residing within the memory of the first security unit, said memory being non volatile (See Moriyasu Col. 10 Paragraph 8 and Col. 7 Paragraph 8 wherein it was implied that the keys were stored in non-volatile memory in order for them to be used to encrypt and decrypt the multiple communications);

encrypting the application key in the first unit based on information comprising said operation key and an encryption algorithm (See Moriyasu Col. 8 Lines 42-50);

sending data comprising the encrypted application key to the second unit (See Moriyasu Col. 8 Lines 42-50);

on each downloading, computing an operation key (K3'+K4) in the second unit based on information specific to the second unit (K3), the transport key (K4) and the diversification algorithm (Multi-Value Function) (See Moriyasu Col. 8 Paragraph 5), the same transport key residing in the non-volatile memory of each second security unit of said set (See Moriyasu Col. 10 Paragraph 8 and Col. 7 Paragraph 8 wherein it was implied that the keys were stored in non-volatile memory in order for them to be used to encrypt and decrypt the multiple communications), said operation key not being stored within the memory of said second unit (See Moriyasu Col. 8 Paragraph 8 and Fig. 10); and

decrypting the encrypted application key in the second unit based on information comprising said operation key and a decryption algorithm which is the inverse of the encryption algorithm (See Moriyasu Col. 8 Paragraph 8).

24. Claim 2 recites sending information specific to the second unit to the first unit before computing the application key in the first unit (See Moriyasu Col. 8 Paragraph 2 and Fig. 10).

25. Claim 18 recites sending the random information, information pertaining to an application key and information specific to the second unit to the first unit by means of a first single command (See Moriyasu Fig. 10 AP Key Request Signal and Col. 7 Paragraph 9 – Col. 8 Paragraph 2).

26. Claim 23 recites sending the encrypted application key and the information pertaining to an application key to the second unit by means of a single second command (See Moriyasu Fig. 10 AP Key Distribution Signal and Col. 8 Lines 42-50).

27. Claim 3 recites sending a random number provided by the second unit to the first unit, before encrypting the application key in the first unit (See Moriyasu Fig. 10 Element K3 and AP Key Request Signal and Col. 7 Paragraph 9 – Col. 8 Paragraph 2).

28. Claim 21 is rejected for the same reasons as claim 18 above.

29. Claim 4 recites sending information pertaining to an application key to the first unit, before encrypting the application key within said first unit (See Moriyasu Col. 8 Paragraph 4).

30. Claim 5 recites choosing the application key to be encrypted based on said information (See Moriyasu Col. 8 Paragraph 4).

31. Claim 22 is rejected for the same reasons as claims 18 and 4 above.

32. Claim 6 recites that the encryption of an application key intended for a second unit is unique (See Moriyasu Col. 8 Paragraph 6 wherein the encryption is based on random numbers and is therefore unique).

33. Claim 7 recites verifying integrity of the data includes the encrypted application key (See Moriyasu Fig. 10 and Col. 7 Paragraph 9 – Col. 8 Paragraph 8 wherein the exchanging of keys to create a key (K3'+K4) for AP key transmission inherently provided integrity verification of the received key).

34. Claim 8 recites sending information pertaining to an application key to the second unit, before decrypting the encrypted application key within said second unit of said set (See Moriyasu Col. 8 Paragraphs 6-8 and Fig. 10).

35. Claim 9 recites storing within the second unit, after decrypting the encrypted application key, said key within said second unit (See Moriyasu Col. 1 Field of the

Invention wherein the point of the invention was to distribute keys to terminals, which implied that the keys would be stored).

36. Claim 10 recites that storing of the application key within the second unit is done based on information pertaining to an application key (See Moriyasu Col. 8 Paragraph 8 and rejection of claim 9 above, wherein it was inherent that storing the AP key was based on the AP key).

37. Claim 11 recites verifying that the application key is authentic (See Moriyasu Fig. 10 and Col. 7 Paragraph 9 – Col. 8 Paragraph 8 wherein the exchanging of keys to create a key (K3'+K4) for AP key transmission inherently provided validation that the received key was authentic).

38. Claim 13 recites that the memory comprises a rewritable memory (See Moriyasu Col. 7 Paragraph 8 wherein it was implied that the storage was rewritable in order to write the keys to the storage unit).

39. Claim 14 recites that a second unit comprises several application keys (See Moriyasu Col. 11 Paragraph 3 wherein a user purchases a CD-ROM and installs it on the users personal terminal. It was inherent that if a user purchased several CD-ROMs and then installed them, the user's terminal would have had multiple keys).

40. Claim 15 recites that the first unit comprises several application keys (See Moriyasu Col. 7 Paragraph 8).

41. Claim 16 recites that after encrypting the application key, erasing the operation key temporarily saved within the second volatile memory of the first unit (See Moriyasu Col. 8 Paragraph 6 wherein it was implied that the key used for encrypting the AP key was erased after encryption because it was not stored in the key management unit).

42. Claim 17 recites that after decrypting the application key, erasing the operation key temporarily saved within the second volatile memory of the first unit (See Moriyasu Col. 8 Paragraph 8 wherein it was implied that the key used for decrypting the AP key was erased after decryption because it was not stored in the key management unit).

43. Claim 19 recites sending the encrypted application key and the information pertaining to an application key to the second unit by means of a single second command (See Moriyasu Col. 8 Lines 42-50).

Claim Rejections - 35 USC § 103

44. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> *(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.*

45. Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Moriyasu as applied to claim 20 above, and further in view of Mollier.

Moriyasu disclosed a system for providing a software key from a remote location to a user terminal (See rejection of claim 20 above), but failed to disclose the system comprising a smartcard.

Mollier teaches a system in which a smartcard, able to provide a key to allow unscrambling of a software program, is provided to a paying user (See Mollier Col. 2 Paragraphs 3-10 and Fig. 1)

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the smartcard of Mollier to the key transferring method of Moriyasu. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide a way for a supplier to rent programs to a user.

Conclusion

46. Claims 2-23 have been rejected.

47. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Epstein (US Patent Number 5,517,567) disclosed a method for providing remote units with a security key, only deviating from the claims in minor, obvious details.

b. Garguilo et al. (US Patent Number 4,935,961) disclosed a method for synchronizing cryptographic keys involving key encrypting keys.

48. Please direct all inquiries concerning this communication to Matthew Henning whose telephone number is (703) 305-0713 until October 21st and (571) 272-3790 thereafter. The examiner can normally be reached Monday-Friday from 9am to 4pm, EST.

If attempts to reach examiner by telephone are unsuccessful, the examiner's acting supervisor, Ayaz Sheikh, can be reached at (703) 305-9648 until October 21st and (571)272-3795 thereafter. The fax phone number for this group is (703) 305-3718.

Any inquiry of general nature or relating to the status of this application or proceeding should be directed to the Group receptionist whose telephone number is (703) 305-3900.

Matthew Henning
Assistant Examiner
Art Unit 2131

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100